

# An improved two-way continuous-variable quantum key distribution with added noise in homodyne detection

Maozhu Sun, Xiang Peng and Hong Guo

CREAM Group, The State Key Laboratory of Advanced Optical Communication Systems and Networks and Institute of Quantum Electronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, PR China

E-mail: xiangpeng@pku.edu.cn, hongguo@pku.edu.cn

**Abstract.** We propose an improved two-way continuous-variable quantum key distribution (CV QKD) protocol by adding proper random noise on the receiver's homodyne detection, the security of which is analysed against general collective attacks. The simulation result under the collective entangling cloner attack indicates that the correlation between two-way channels decreases the secret key rate relative to the uncorrelated channels. Importantly, the added noise in detection is beneficial for the secret key rate and the tolerable excess noise of this two-way protocol. With the reasonable reconciliation efficiency of 90%, the two-way CV QKD with added noise allows the distribution of secret keys over 60 km fibre distance.

PACS numbers: 03.67.Dd, 03.67.Hk

## 1. Introduction

Quantum key distribution can enable two authentic parties, the sender (Alice) and the receiver (Bob), to obtain unconditional secret keys without restricting the power of the eavesdropper (Eve) [1, 2]. On the premise of unconditional security, the higher key rate and the longer distance are constantly pursued [3, 4]. To enhance the tolerable excess noise of the continuous-variable quantum key distribution (CV QKD) [5, 6], the two-way CV QKD protocols are proposed [7, 8], where Bob initially sends a mode to Alice, and Alice encodes her information by applying a random displacement operator to the received mode and then sends it back to Bob. Bob detects both his original mode and received mode to decode Alice's modulations. Although the two-way CV QKD protocols can remarkably enhance the tolerable excess noise [7, 8], it needs to implement the tomography of the quantum channels to analyze the security under general collective attack [7], which is complicated in practice. Therefore, we proposed a feasible modified two-way protocol by replacing the displacement operation of the original two-way protocol with a passive operation on Alice's side [9]. However, the source noise [10, 11, 12, 13, 14] and both detection efficiency and detection noise [15, 16] on Bob's side are not considered in the modified protocol.

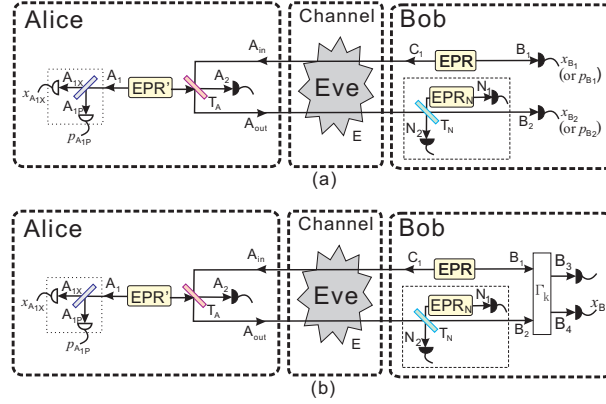
It has been proved that adding a proper noise on Bob's detection side in one-way CV QKD can enhance the tolerable excess noise and the secret key rate in reverse reconciliation [12, 17, 18, 19, 20, 21]. This idea has been applied to the original two-way protocol in [22], while the scheme did not consider the correlation between the two channels. The correlated noise affects the secret key rate [23, 24]. In this paper, we apply the idea of adding noise to our modified two-way protocol  $\text{Hom}_M^2$  [9] to enhance the tolerable excess noise and the secret key rate. Considering the correlation between the channels, the security of the two-way CV QKD with added noise against entangling cloner collective attacks [25, 26] is analysed and numerically simulated.

## 2. The two-way CV QKD with added noise in homodyne detection

The entanglement-based (EB) scheme of the two-way CV-QKD protocol  $\text{Hom}_N^2$  with added detection noise is shown in Figure 1(a), where the dashed box at  $B_2$  is the added noise and the other part is our original two-way protocol  $\text{Hom}_M^2$  [9]. The added noise is equivalent to an EPR pair with the variance of  $V_N$  coupled into the channel by a beam splitter with the transmittance of  $T_N$ . The protocol  $\text{Hom}_N^2$  is described as follows.

*Step one.* Bob initially keeps one mode  $B_1$  of an EPR pair with the variance of  $V$  while sending the other mode  $C_1$  to Alice through the forward channel.

*Step two.* Alice measures one mode  $A_1$  of her EPR pair (variance:  $V_A$ ) to get the variables  $\{x_{A_{1X}}, p_{A_{1P}}\}$  with a heterodyne detection, and couples the other mode of her EPR pair with the received mode  $A_{in}$  from Bob by a beam splitter (transmittance:  $T_A$ ). One output mode  $A_2$  of the beam splitter is measured with homodyne detection and the other output mode  $A_{out}$  is sent back to Bob through the backward channel.



**Figure 1.** (a) The EB scheme of  $\text{Hom}_N^2$  protocol. Bob keeps one half of the EPR pair (EPR) and sends the other half to Alice. Alice measures one mode of her EPR pair (EPR') and one mode  $A_2$  from a beam splitter  $T_A$ . The other mode from this beam splitter is returned back to Bob. The letters (e.g.  $B_1$ ) beside arrows: the mode at the arrow; E: Eve's whole mode; the dashed box at  $A_1$ : the heterodyne detection; the dashed box at  $B_2$ : the added noise. (b) The equivalent scheme to Figure 1 (a) with postprocessing. Bob uses a symplectic transformation  $\Gamma_k$  to change the modes  $B_2$  and  $B_1$  into  $B_3$  and  $B_4$ .

*Step three.* With a beam splitter (transmittance:  $T_N$ ), Bob couples another EPR pair (variance:  $V_N$ ) which is equivalent to the added noise with his received mode. The two modes  $N_1$  and  $N_2$  of this EPR pair are measured. Bob performs homodyne detections on both modes  $B_1$  and  $B_2$  to get the variables  $x_{B_1}$  (or  $p_{B_1}$ ) and  $x_{B_2}$  (or  $p_{B_2}$ ), respectively.

*Step four.* Alice and Bob implement the reconciliation and privacy amplification [27, 28]. In this step, the measurement values of the modes  $B_2$ ,  $B_1$ ,  $A_2$ ,  $A_1$ ,  $N_2$  and  $N_1$  are used to estimate the channel's parameters and Bob uses  $x_B = x_{B_2} - kx_{B_1}$  ( $p_B = p_{B_2} + kp_{B_1}$ ) to construct the optimal estimation to Alice's corresponding variables  $x_{A_{1X}}$  ( $p_{A_{1P}}$ ), where  $k$  is the channel's total transmittance.

The prepare-and-measure (PM) scheme of the two-way protocol can be equivalent to the EB scheme. In fact, Alice heterodyning one half of the EPR pair at  $A_1$  is equivalent to remotely preparing a coherent state, and Bob performing homodyne detection on one half of the EPR pair at  $B_1$  is equivalent to remotely preparing a squeezed state [25]. The homodyne detection preceded by an EPR pair coupled by a beam splitter at  $B_2$  is equivalent to Bob's real homodyne detection with efficiency  $T_N$  and electronic noise [17]. Note that  $x$  and  $p$  quadratures are randomly measured in homodyne detection and only  $x$  quadrature is analysed in the following.

### 3. The analysis of the security against general collective attack

First, we show that the Gaussian attack is optimal to the two-way protocol  $\text{Hom}_N^2$  in general collective attack. In Figure 1(a), since all modes of Alice and Bob are measured, Eve can get the purification of the state of Alice and Bob. In addition, the  $x$  and

$p$  quadratures of Alice and Bob's modes are not mixed via heterodyne or homodyne detection and Alice and Bob use the second-order moments of the quadratures to bound Eve's information. Therefore, the two-way protocol  $\text{Hom}_N^2$  can satisfy the requirement of optimality of Gaussian collective attack (i.e., continuity, invariance under local Gaussian unitary and strong subadditivity) [29]. When the corresponding covariance matrix of the state  $B_2B_1N_2N_1A_2A_1$  is known for Alice and Bob, the Gaussian attack is optimal [30, 31, 32, 33]. Therefore, only Eve's Gaussian collective attack is needed to be considered in the following security analysis.

In Figure 1(a), the secret key rate of the two-way protocol  $\text{Hom}_N^2$  in reverse reconciliation is [16, 34, 35, 36]

$$\begin{aligned} K_R &= \beta I(B : A) - I(B : E) \\ &= \frac{1}{2} \beta \log_2 \frac{V_{A^M}}{V_{A^M|x_B}} - S(E) + S(E|x_B), \end{aligned} \quad (1)$$

where  $\beta$  is the reconciliation efficiency,  $I(B : A)$  [ $I(B : E)$ ] is the mutual information between Bob and Alice (Eve),  $V_{A^M}$  and  $V_{A^M|x_B}$  are Alice's variance and conditional variance,  $S(E)$  and  $S(E|x_B)$  are Eve's von Neumann entropy and conditional von Neumann entropy on Bob's data, respectively. In the following,  $S(E)$  and  $S(E|x_B)$  are calculated by the methods in [37].

For Gaussian state, the entropy can be calculated from its corresponding covariance matrix [38]. Since the state  $B_2B_1N_2N_1A_2A_1E$  is a pure state, then  $S(E) = S(B_2B_1N_2N_1A_2A_1)$ . The corresponding covariance matrix of the state  $B_2B_1N_2N_1A_2A_1$  is

$$\Gamma_{B_2B_1N_2N_1A_2A_1} = \begin{pmatrix} \gamma_{B_2} & C_1 & C_2 & C_3 & C_4 & C_5 \\ C_1 & V\mathbb{I} & C_6 & 0 & C_7 & 0 \\ C_2 & C_6 & \gamma_{N_2} & C_8 & C_9 & C_{10} \\ C_3 & 0 & C_8 & V_N\mathbb{I} & 0 & 0 \\ C_4 & C_7 & C_9 & 0 & \gamma_{A_2} & C_{11} \\ C_5 & 0 & C_{10} & 0 & C_{11} & V_A\mathbb{I} \end{pmatrix}, \quad (2)$$

where  $\mathbb{I}$  is a  $2 \times 2$  identity matrix, the diagonal elements correspond to the variances of  $x$  and  $p$  quadratures of the modes  $B_2$ ,  $B_1$ ,  $N_2$ ,  $N_1$ ,  $A_2$  and  $A_1$  in turn, e.g.  $\gamma_{B_2} = \text{diag}(\langle x_{B_2}^2 \rangle, \langle p_{B_2}^2 \rangle)$ , and the nondiagonal elements correspond to the covariances between modes, e.g.  $C_1 = \text{diag}(\langle x_{B_2}x_{B_1} \rangle, \langle p_{B_2}p_{B_1} \rangle)$ . Therefore, Eve's entropy [39]

$$S(E) = \sum_{i=1}^6 G(\lambda_i) = \sum_{i=1}^6 G(f_{\lambda_i}(\alpha_{mn})), \quad (3)$$

where  $G(\lambda_i) = \frac{\lambda_i+1}{2} \log \frac{\lambda_i+1}{2} - \frac{\lambda_i-1}{2} \log \frac{\lambda_i-1}{2}$ , and  $\lambda_i = f_{\lambda_i}(\alpha_{mn})$  is the symplectic eigenvalue of  $\Gamma_{B_2B_1N_2N_1A_2A_1}$  which is the function of the element  $\alpha_{mn}$  of  $\Gamma_{B_2B_1N_2N_1A_2A_1}$  [40, 41], seen in Appendix A.

Bob uses  $x_B = x_{B_2} - kx_{B_1}$  to estimate Alice's variable, which is equivalent to that Bob uses a symplectic transformation  $\Gamma_k$  to change the modes  $B_2$  and  $B_1$  into the modes  $B_4$  and  $B_3$  where the  $x$  quadrature of the mode  $B_4$  is  $x_{B_4} = x_B = x_{B_2} - kx_{B_1}$  [9], as

shown in Figure 1(b). Since Figure 1(b) is equivalent to Figure 1(a) with postprocessing, we use Figure 1(b) to calculate  $S(E|x_B)$  in the following.

After the symplectic transformation  $\Gamma_k$ , the corresponding covariance matrix of the mode  $B_4B_3N_2N_1A_2A_1$  is

$$\Gamma_{B_4B_3N_2N_1A_2A_1} = [\Gamma_k \oplus \mathbb{I}_4] \Gamma_{B_2B_1N_2N_1A_2A_1} [\Gamma_k \oplus \mathbb{I}_4]^T, \quad (4)$$

where  $\mathbb{I}_4 = \oplus_1^4 \mathbb{I}$ ,  $\Gamma_k$  is a continuous-variable C-NOT gate [29, 42, 43]

$$\Gamma_k = \begin{pmatrix} 1 & 0 & -k & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & k & 0 & 1 \end{pmatrix}. \quad (5)$$

Since the state  $B_3N_2N_1A_2A_1E$  is a pure state when Bob gets  $x_B$  by measuring the modes  $B_4$ , then  $S(E|x_B) = S(B_3N_2N_1A_2A_1|x_B)$ . The corresponding covariance matrix of the state  $B_3N_2N_1A_2A_1$  conditioned on  $x_B$  is [29, 44]

$$\Gamma_{B_3N_2N_1A_2A_1}^{x_B} = \gamma_{B_3N_2N_1A_2A_1} - C_{B_4} [X_x \gamma_{B_4} X_x]^{MP} C_{B_4}, \quad (6)$$

where  $\gamma_{B_3N_2N_1A_2A_1}$  and  $\gamma_{B_4}$  are the corresponding reduced matrixes of the states  $B_3N_2N_1A_2A_1$  and  $B_4$  in  $\Gamma_{B_4B_3N_2N_1A_2A_1}$ , respectively,  $C_{B_4}$  is their correlation matrix,  $X_x = \text{diag}(1, 0)$  and  $MP$  denotes the inverse on the range. Therefore, we have

$$S(E|x_B) = \sum_{i=1}^5 G(\lambda'_i) = \sum_{i=1}^5 G(f_{\lambda'_i}(\alpha'_{mn})), \quad (7)$$

where  $\lambda'_i = f_{\lambda'_i}(\alpha'_{mn})$  is the symplectic eigenvalue of  $\Gamma_{B_3N_2N_1A_2A_1}^{x_B}$  which is the function of the element  $\alpha'_{mn}$  of  $\Gamma_{B_3N_2N_1A_2A_1}^{x_B}$  [40, 41], seen in Appendix A.

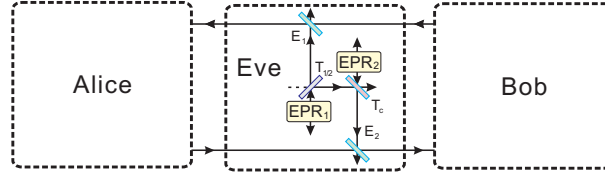
By substituting equations (3) and (7) into equation (1), the secret key rate is obtained

$$K_R = \frac{1}{2} \beta \log_2 \frac{V_{AM}}{V_{AM|x_B}} - \sum_{i=1}^6 G(f_{\lambda_i}(\alpha_{mn})) + \sum_{i=1}^5 G(f_{\lambda'_i}(\alpha'_{mn})). \quad (8)$$

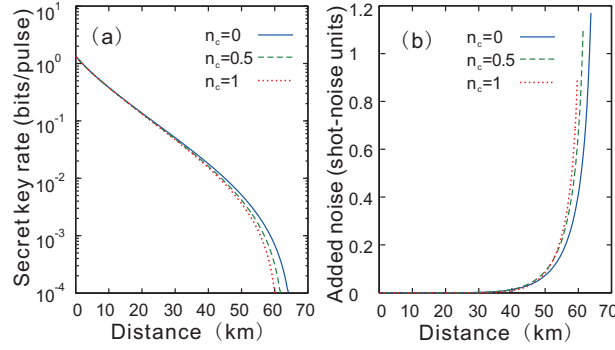
In experiment, Alice and Bob can calculate the element  $\alpha_{mn}$  and  $\alpha'_{mn}$  of equations (2) and (6) by the measurement values of the modes  $B_2$ ,  $B_1$ ,  $N_2$ ,  $N_1$ ,  $A_2$  and  $A_1$ . Therefore, according to equation (8), the secret key rate in general collective attack is obtained without the assumption of channels. The analytic representations of equation (8) is too complex to give here. We give a numerical simulation in the following.

#### 4. Numerical simulation and discussion of collective entangling cloner attacks on correlated and uncorrelated channels

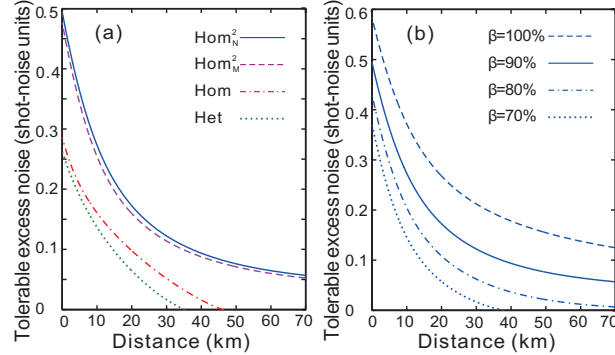
For simplicity in numerical simulation, when there is no Eve, the forward and the backward channels are assumed to be independent with the identical transmittances  $T$  and noises referred to the input  $\chi = \varepsilon + (1 - T)/T$ , where  $\varepsilon$  is the channel excess noises referred to the input. It is equivalent to Eve implementing two independent collective entangling cloner attacks which are a Gaussian collective attack investigated in detail



**Figure 2.** The EB scheme of  $\text{Hom}_N^2$  protocol against entangling cloner attacks on correlated channels.  $E_1, E_2$ : the modes introduced into the channels;  $T_{1/2}$ : half beam splitter;  $T_c$ : beam splitter. Alice and Bob are the same as Figure 1(a).

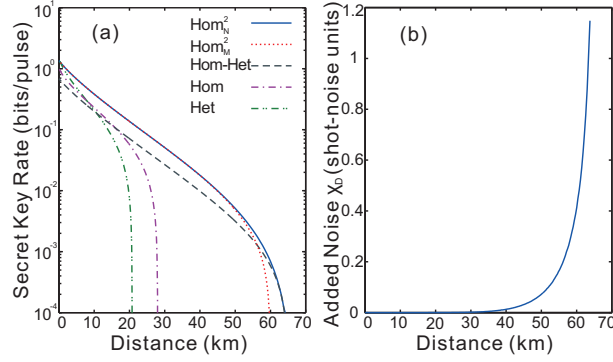


**Figure 3.** (a) Secret key rate as a function of the transmission distance for  $\text{Hom}_N^2$  protocol, where  $\varepsilon = 0.06$ ,  $\beta = 90\%$ ,  $T_A = 0.8$ ,  $V_A = V = 20$  and  $n_c = 0, 0.5, 1$ . (b) Optimal choice of the added noise  $x_D$ .



**Figure 4.** (a) Tolerable excess noise as a function of the transmission distance for  $\text{Hom}_N^2$ ,  $\text{Hom}_M^2$ ,  $\text{Hom}$  and  $\text{Het}$  protocols, where  $\beta = 90\%$ . (b) Tolerable excess noise as a function of the transmission distance for  $\text{Hom}_N^2$ , where  $\beta = 100\%, 90\%, 80\%, 70\%$ . The curves of (a) and (b) are plotted for  $n_c = 0$ ,  $T_A = 0.8$ , and  $V_A = V = 20$ .

in [45, 46]. When Eve implements more complicated two-mode attack, the correlation between the two channels is induced. Figure 2 shows that Eve implements two correlated entangling cloner attacks. On condition that Eve introduces the equivalent variances of the modes  $E_1$  and  $E_2$  into the two channels, the noise referred to the input of the backward channel is  $\chi_2 = \chi + 2n_c\sqrt{T_A T}\varepsilon$ , where the second item on the right-hand side is induced extra by the correlation between the two channels, i.e., the part of the mode introduced into the backward channel correlating with the forward channel interferes with the mode from Alice,  $n_c = \sqrt{1 - T_c}$  is the coefficient representing the degree of the



**Figure 5.** (a) Secret key rate as a function of the transmission distance for  $\text{Hom}_N^2$ ,  $\text{Hom}_M^2$ , Hom-Het, Hom and Het protocols where  $n_c = 0$ ,  $\varepsilon = 0.06$ ,  $\beta = 90\%$ ,  $T_A = 0.8$  and  $V_A = V = 20$ . (b) Optimal choice of the added noise  $\chi_D$ .

correlation, e.g.,  $n_c = 0$  represents that the two channels are uncorrelated. The added noise is  $\chi_D = (1 - T_N)V_N/T_N$ . We can calculate the elements of equation (2)

$$\begin{aligned}
\gamma_{B_2} &= \{V_N - T_N V_N + T T_N [V_A - T_A V_A + T T_A (V + \chi) + \chi_2]\} \mathbb{I}, \\
\gamma_{N_2} &= \{T_N V_N + T(1 - T_N)[V_A - T_A V_A + T T_A (V + \chi) + \chi_2]\} \mathbb{I}, \\
\gamma_{A_2} &= [T_A V_A + T(1 - T_A)(V + \chi)] \mathbb{I}, \\
C_1 &= -\eta C_6 = T \sqrt{T_A T_N (V^2 - 1)} \sigma_z, \\
C_2 &= \sqrt{(1 - T_N) T_N} \{V_N - T[V_A - T_A V_A + T T_A (V + \chi) + \chi_2]\} \mathbb{I}, \\
C_3 &= \frac{1}{\eta} C_8 = \sqrt{(1 - T_N)(V_N^2 - 1)} \sigma_z, \\
C_4 &= -\eta C_9 = \sqrt{T(1 - T_A) T_N} \left[ \sqrt{T_A} V_A - T \sqrt{T_A} (V + \chi) - n_c \sqrt{T} \varepsilon \right] \mathbb{I}, \\
C_5 &= -\eta C_{10} = \sqrt{T(1 - T_A) T_N (V_A^2 - 1)} \sigma_z, \\
C_7 &= -\sqrt{T(1 - T_A)(V^2 - 1)} \sigma_z, \\
C_{11} &= \sqrt{T_A (V_A^2 - 1)} \sigma_z,
\end{aligned} \tag{9}$$

and

$$I(B:A) = \frac{1}{2} \log_2 \frac{T^2 T_A F + T(V_A - T_A V_A + \chi_2) + \chi_D}{T(1 - T_A + \chi_2) + T^2 T_A F + \chi_D}, \tag{10}$$

where  $\sigma_z = \text{diag}(1, -1)$ ,  $\eta = \sqrt{T_N/(1 - T_N)}$ ,  $F = 2V - 2\sqrt{V^2 - 1} + \chi$ . The typical fiber channel loss is assumed to be 0.2 dB/km.  $V$  and  $\varepsilon$  are in shot-noise units. Substituting equations (9) and (10) into equation (8), the optimal secret key rate  $K_R$  and the optimal tolerable excess noise  $\varepsilon$  of the two-way protocol  $\text{Hom}_N^2$  can be obtained by adjusting the added noise  $\chi_D$ .

Figure 3(a) shows the secret key rate as a function of the transmission distance for  $\text{Hom}_N^2$  protocol with different  $n_c$ . Considering the practical experiment [15, 16, 47], we choose  $\varepsilon = 0.06$ ,  $\beta = 90\%$ ,  $T_A = 0.8$ ,  $V_A = V = 20$  and  $n_c = 0, 0.5, 1$ . To make  $K_R$  optimal, the proper added noise  $\chi_D$  is chosen, as shown in Figure 3(b). In Figure 3(a), the simulation result indicates that the distance of the secret key distribution decreases

with the increase of  $n_c$ , which indicates that the correlation between the channels is beneficial for Eve. Figure 3(b) shows that the optimal added noise decreases with the decrease of  $n_c$ .

When  $n_c = 0$ , the two channels are uncorrelated, which is equivalent to Eve implementing two independent Gaussian cloner attacks. For comparison, the heterodyne protocol (Het) [48] and the homodyne protocol (Hom) [36] of one-way CV-QKD protocol with coherent state and the original modified two-way protocols  $\text{Hom}_M^2$  and  $\text{Hom-Het}_M$  [9] are also given in figures. 4(a) and 5(a). Figure 4(a) shows the tolerable excess noise as a function of the transmission distance, where  $V_A = V = 20$ ,  $T_A = 0.8$ ,  $\beta = 90\%$  and  $n_c = 0$ . The proper added noise  $\chi_D$  is chosen to make  $\varepsilon$  of  $\text{Hom}_N^2$  protocol optimal. The numerical simulation result indicates that the tolerable excess noise of the two-way protocol with added noise is more than that without added noise and surpasses that of the one-way CV-QKD protocol. Therefore, it indicates that properly added noise is useful to enhance  $\varepsilon$  in the two-way protocol. Figure 4(b) shows the tolerable excess noise  $\varepsilon$  of  $\text{Hom}_N^2$  protocol with different  $\beta$ , which indicates that the tolerable excess noise  $\varepsilon$  increases with the increase of  $\beta$ .

Figure 5(a) shows the secret key rate as a function of the transmission distance, where  $V = V_A = 20$ ,  $T_A = 0.8$ ,  $\varepsilon = 0.06$ ,  $\beta = 90\%$  and  $n_c = 0$ . To make the secret key rate of  $\text{Hom}_N^2$  optimal, the proper added noise  $\chi_D$  is chosen, as shown in Figure 5(b). In Figure 5(a), the simulation result indicates that the two-way protocol with added noise has higher secret key rate than that without added noise. Especially, the achievable transmission distance of the two-way protocol  $\text{Hom}_N^2$  is over 60 km when  $\beta$  is 90%, which is much longer than that of the one-way protocol. The reason is that the added noise not only lowers the mutual information between Alice and Bob, but also lowers that between Bob and Eve. When the effect on Eve is more than that on Alice and Bob, the secret key rate is enhanced.

## 5. Conclusion

In conclusion, we improve the two-way CV-QKD protocol by adding a proper noise on Bob's detection side. The security of the two-way CV-QKD protocol with added noise in homodyne detection against general collective attack is analysed. The numerical simulation under the collective entangling cloner attack is given for the correlated and the uncorrelated channels. The simulation result indicates that the secret key rate for the correlated channel is lower than that for the the uncorrelated channel when Eve inputs equivalent variance of the modes into the two channels. In addition, the properly added noise is beneficial for enhancing the secret key rate and the tolerable excess noise of the two-way CV QKD. The optimal tolerable excess noise of the two-way CV QKD with added noise is much more than that of the one-way CV QKD. With the reasonable reconciliation efficiency of 90%, the two-way CV QKD with added noise allows the distribution of secret keys over 60 km fibre distance, which is difficult to reach for the one-way CV-QKD protocols with Gaussian modulation in experiment.



## Acknowledgments

This work is supported by the Key Project of National Natural Science Foundation of China (Grant No. 60837004 and 61101081), National Hi-Tech Research and Development (863) Program.

## Appendix A. The calculation of eigenvalues

We use  $\alpha''_{mn}$  to denote the elements of the corresponding covariance matrix  $\Gamma_n$  of a  $n$ -mode state. The symplectic invariants  $\{\Delta_{n,j}\}$  of  $\Gamma_n$  for  $j = 1, \dots, n$  are defined as [40]

$$\Delta_{n,j} = M_{2j}(\Omega\Gamma_n), \quad (\text{A.1})$$

where  $\Omega = \oplus_1^n i\sigma_y$  ( $\sigma_y$  standing for the  $y$  Pauli matrix) and  $M_{2j}(\Omega\Gamma)$  is the principal minor of order  $2j$  of the  $2n \times 2n$  matrix  $\Omega\Gamma$  which is the sum of the determinants of all the  $2j \times 2j$  submatrices of  $\Omega\Gamma_n$  [40, 41].

The symplectic eigenvalues of the matrix corresponding to a four-mode state are the solution of the four-order equation on the symplectic invariants [9, 29, 40]

$$\begin{aligned} f_{1,2}^2(\alpha''_{mn}) &= \frac{\Delta_{41}}{4} - \frac{1}{2}\sqrt{\zeta + \Theta} \pm \frac{1}{2}\sqrt{2\zeta - \Theta - \frac{\Delta_{41}^3 - 4\Delta_{41}\Delta_{42} + 8\Delta_{43}}{4\sqrt{\zeta + \Theta}}}, \\ f_{3,4}^2(\alpha''_{mn}) &= \frac{\Delta_{41}}{4} + \frac{1}{2}\sqrt{\zeta + \Theta} \pm \frac{1}{2}\sqrt{2\zeta - \Theta + \frac{\Delta_{41}^3 - 4\Delta_{41}\Delta_{42} + 8\Delta_{43}}{4\sqrt{\zeta + \Theta}}}, \end{aligned} \quad (\text{A.2})$$

where

$$\begin{aligned} \zeta &= \frac{\Delta_{41}^2}{4} - \frac{2\Delta_{42}}{3}, \quad \Theta = \frac{2^{\frac{1}{3}}H}{3J} + \frac{J}{3 \cdot 2^{\frac{1}{3}}}, \\ H &= \Delta_{4,2}^2 - 3\Delta_{4,1}\Delta_{4,3} + 12\Delta_{4,4}, \quad J = \left(L + \sqrt{L^2 - 4H^3}\right)^{\frac{1}{3}}, \\ L &= 2\Delta_{4,2}^3 - 9\Delta_{4,1}\Delta_{4,2}\Delta_{4,3} + 27\Delta_{4,3}^2 + 27\Delta_{4,1}^2\Delta_{4,4} - 72\Delta_{4,2}\Delta_{4,4}. \end{aligned} \quad (\text{A.3})$$

From equation (2), the covariance matrix  $\Gamma_{N_1N_2B_2B_1A_2A_1}$  of the modes  $N_1N_2B_2B_1A_2A_1$  can be obtained by permuting the corresponding elements of  $\Gamma_{B_2B_1N_2N_1A_2A_1}$ . Applying a unitary transformation  $S = \mathbb{I} \oplus \Gamma_{T_N} \oplus \mathbb{I} \oplus \mathbb{I}$  to equation (2), we can obtain

$$S^T \Gamma_{N_1N_2B_2B_1A_2A_1} S = \begin{pmatrix} \Gamma_{N_1N_2'} & 0 \\ 0 & \Gamma_{B_2'B_1A_2A_1} \end{pmatrix}, \quad (\text{A.4})$$

where

$$\begin{aligned} \Gamma_{T_N} &= \begin{pmatrix} \sqrt{T_N}\mathbb{I} & \sqrt{1-T_N}\mathbb{I} \\ -\sqrt{1-T_N}\mathbb{I} & \sqrt{T_N}\mathbb{I} \end{pmatrix}, \quad \Gamma_{N_1N_2'} = \begin{pmatrix} V_N\mathbb{I} & \sqrt{V_N^2-1}\sigma_z \\ \sqrt{V_N^2-1}\sigma_z & V_N\mathbb{I} \end{pmatrix}, \\ \Gamma_{B_2'B_1A_2A_1} &= \begin{pmatrix} \gamma'_{B_2} & C'_1 & C'_4 & C'_5 \\ C'_1 & V\mathbb{I} & C_7 & 0 \\ C'_4 & C_7 & \gamma_{A_2} & C_{11} \\ C'_5 & 0 & C_{11} & V_A\mathbb{I} \end{pmatrix}, \end{aligned} \quad (\text{A.5})$$

and  $\gamma'_{B_2} = [\gamma_{B_2} - (1 - T_N)V_N]/T_N$ ,  $C'_i = C_i/\sqrt{T_N}$  for  $i = 1, 4, 5$ . Therefore, the eigenvalues of  $\Gamma_{B_2B_1N_2N_1A_2A_1}$  are  $\lambda_i = f_{\lambda_{1,2,3,4}}(\alpha_{mn})$ , 1, 1, where  $f_{\lambda_{1,2,3,4}}(\alpha_{mn})$  are the eigenvalues of  $\Gamma_{B'_2B_1A_2A_1}$  given by equation (A.2).

The symplectic invariants of  $\Gamma_{B_2B_1N_2N_1A_1A_2}^{xB}$  are denote as  $\Delta_{5j}$  for  $j=1\dots 5$ . It can be proved that  $1 - \Delta_{51} + \Delta_{52} - \Delta_{53} + \Delta_{54} - \Delta_{55} = 0$ . Therefore, one of the eigenvalues of  $\Gamma_{B_1A_1A_2B_2N_2N_1}^{xB}$  is 1 and the others have the same forms of equation (A.2), which needs the replacement  $\Delta_{41} = \Delta_{51} - 1$ ,  $\Delta_{42} = \Delta_{52} - \Delta_{51} + 1$ ,  $\Delta_{43} = \Delta_{54} - \Delta_{55}$ ,  $\Delta_{44} = \Delta_{55}$ .

## References

- [1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
- [2] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Proceedings* (New York: IEEE Press) pp 175–9
- [3] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
- [4] Blandino R, Leverrier A, Barbieri M, Etesse J, Grangier P and Tualle-Brouri R 2012 *Phys. Rev. A* **86** 012327
- [5] Hillery M 2000 *Phys. Rev. A* **61** 022309
- [6] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
- [7] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 *Nature Phys.* **4** 726
- [8] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
- [9] Sun M, Peng X, Shen Y and Guo H 2011 arXiv:1110.1818v4
- [10] Filip R 2008 *Phys. Rev. A* **77** 022310
- [11] Usenko V C and Filip R 2010 *Phys. Rev. A* **81** 022318
- [12] Weedbrook C, Pirandola S, Lloyd S and Ralph T C 2010 *Phys. Rev. Lett.* **105** 110501
- [13] Shen Y, Yang J and Guo H 2009 *J. Phys. B: At. Mol. Opt. Phys.* **42** 235506
- [14] Shen Y, Peng X, Yang J and Guo H 2011 *Phys. Rev. A* **83** 052304
- [15] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 *Phys. Rev. A* **72** 050303
- [16] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W and Grangier P 2007 *Phys. Rev. A* **76** 042305
- [17] García-Patrón R and Cerf N J 2009 *Phys. Rev. Lett.* **102** 130501
- [18] Weedbrook C, Pirandola S and Ralph T C 2012 *Phys. Rev. A* **86** 022318
- [19] Pirandola S, García-Patrón R, Braunstein S L and Lloyd S 2009 *Phys. Rev. Lett.* **102** 050503
- [20] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 012332
- [21] Renes J M and Smith G 2007 *Phys. Rev. Lett.* **98** 020502
- [22] Wang M and Pan W 2010 *Phys. Lett. A* **374** 2434
- [23] Huang P, Zhu J, He G and Zeng G 2012 *J. Phys. B: At. Mol. Opt. Phys.* **45** 135501
- [24] Huang P, He G, Lu Y and Zeng G 2011 *Phys. Scr.* **83** 015005
- [25] Grosshans F, Cerf N J, Wenger J, Brouri R and Grangier P 2003 *Quantum Inf. Comput.* **3** 535
- [26] Weedbrook C, Grosse N B, Symul T, Lam P K and Ralph T C 2008 *Phys. Rev. A* **77** 052313
- [27] Assche G V 2006 *Quantum Cryptography and Secret-Key Distillation* (Cambridge: Cambridge University Press)
- [28] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 *IEEE Trans. Inf. Theory* **41** 1915
- [29] García-Patrón R 2007 Ph.D. thesis, Université Libre de Bruxelles
- [30] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
- [31] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502
- [32] Wolf M M, Giedke G and Cirac J I 2006 *Phys. Rev. Lett.* **96** 080502

- [33] Leverrier A and Grangier P 2010 *Phys. Rev. A* **81** 062314
- [34] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 *Phys. Rev. A* **77** 042325
- [35] Holevo A S 1973 *Probl. Inf. Transm.* **9** 177
- [36] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
- [37] Lu H, Fung C F, Ma X and Cai Q 2011 *Phys. Rev. A* **84** 042344
- [38] Serafini A, Illuminati F and De Siena S 2004 *J. Phys. B: At. Mol. Opt. Phys.* **37** L21
- [39] Holevo A S, Shor M and Hirota O 1999 *Phys. Rev. A* **59** 1820
- [40] Serafini A 2006 *Phys. Rev. Lett.* **96** 110402
- [41] Pirandola S, Serafini A and Lloyd S 2009 *Phys. Rev. A* **79** 052327
- [42] Yoshikawa J I, Miwa Y, Huck A, Andersen U L, van Loock P and Furusawa A 2008 *Phys. Rev. Lett.* **101** 250501
- [43] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
- [44] Eisert J and Plenio M B 2003 *Int. J. Quant. Inf.* **1** 479
- [45] Pirandola S, Braunstein S L and Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504
- [46] Holevo A S 2007 *Probl. Inf. Transm.* **43** 1
- [47] Symul T, Alton D J, Assad S M, Lance A M, Weedbrook C, Ralph T C and Lam P K 2007 *Phys. Rev. A* **76** 030303
- [48] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504